GIPL JC68 AUG 22 2003 PATENT & TRADEMARK OFFICE

PAT-NO: JP02000076139A

DOCUMENT-IDENTIFIER: JP 2000076139 A

TITLE: PORTABLE INFORMATION STORAGE MEDIUM

PUBN-DATE: March 14, 2000

INVENTOR-INFORMATION:

NAME	COUNTRY
TANNO, MASAAKI	N/A
TAKEDA, TADAO	N/A
BAN, KOJI	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
NIPPON TELEGR & TELEPH CORP <NTT>	N/A

APPL-NO: JP10243380

APPL-DATE: August 28, 1998

INT-CL (IPC): G06F012/14, G06K019/073

ABSTRACT:

PROBLEM TO BE SOLVED: To erase secret information and to preserve required information upon detecting a physical attack from the outside.

SOLUTION: A sensor element 2 detects the physical attack from the outside. A first memory element 3 is a writable/readable memory and a second memory element 5 is a read-only memory capable of white only once. A voltage monitoring means 8 monitors the output voltage of a battery 7. When the physical attack is detected by the sensor element 2 or when the output voltage

abnormality of the battery 7 is detected by a voltage monitoring mechanism 8, a
memory control mechanism 6 reads information to be preserved from the memory
element 3, writes it in the memory element 5 and erases the secret information
stored in the memory element 3.

COPYRIGHT: (C)2000,JPO

* NOTICES *

Japan Patent Office is not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[The technical field to which invention belongs] this invention relates to the technology which defends important storage information from an unjust attack while checking analyzing storage information, such as an IC card, unjustly in detail about the security of the portable small information-storage medium represented by the IC card.
[0002]
[Description of the Prior Art] In order to protect storage information from the physical attack unjust as an information-storage medium which memorizes extra sensitive information etc. conventionally, what builds in a physical security mechanism is proposed. as a typical example, there is muABYSS (bibliography: -- S.H.Weigart, "Physical security for the mu ABYSS system", and Proc.1987 IEEE Symp.onSecurity and Privacy, Oakland, CA, pp.52-58 and April 1987) of U.S. IBM
[0003] This muABYSS cannot observe the interior of a module, unless the whole module is wrapped in the metal thin line in the shape of a cocoon and a metal thin line is cut. When a metal thin line is cut, the security mechanism built in the module detects resistance change of a metal thin line, and eliminates extra sensitive information immediately. Disclosure of extra sensitive information is prevented by this. Sensing of the attack from the outside of the information-storage medium which contains other security mechanisms is performing operation which eliminates important information.
[0004]
[Problem(s) to be Solved by the Invention] As mentioned above, it becomes impossible to read extra sensitive information with being natural even if the security mechanism of the conventional information-storage medium performs regular information read-out operation to an information-storage medium after a security mechanism detects an attack, in order to prevent the disclosure by eliminating extra sensitive information. Since the balance data in a card would be eliminated if a security mechanism operates according to intentionally, negligence, or accident when the carried type information-storage medium which contained such a security mechanism is applied to a prepaid card or a cybermoney card, there was a trouble that monetary value of a card could not be restored. Moreover, the built-in cell was exhausted and there was also a trouble that indispensable data were lost. Such a problem will not have the basis of the balance data fed into a new prepaid card in case the prepaid card damaged according to a cell piece, accident, etc. is exchanged at the window, and any of a card employment company and a user they are will suffer money-damage. this invention aims at offering the carried type information-storage medium which can save required information while it eliminates extra sensitive information, when it is made in order to solve the above-mentioned technical problem, and the physical attack from the outside is detected. Moreover, when the attack on a built-in cell and exhaustion of a cell are detected, while eliminating extra sensitive information, it aims at offering the carried type information-storage medium which can save required information.
[0005]
[Means for Solving the Problem] The carried type information-storage medium of this invention The sensor element according to claim 1 which detects the physical attack from the outside like (2), The 1st memory device (3) in which write-in read-out is possible, and the 2nd memory device only for read-out which can be written in only at once (5), It has the memory control means (6) interlocked with the response of a sensor element. the above-mentioned memory control means When a physical attack is detected by the sensor element, while reading the information which should be saved from the 1st memory device and writing in the 2nd memory device, the extra sensitive information memorized by the 1st memory device is eliminated. Thus, since memory control means eliminate the extra sensitive information memorized by the 1st memory device while they read the information which should be saved from the 1st memory

device and write it in the 2nd memory device, when a physical attack is detected by the sensor element, they can reconcile prevention of leakage of secrets and preservation of required information. Moreover, it has a voltage surveillance means (8) according to claim 2 to supervise the output voltage of the cell for electric power supplies (7), and this cell like, and the above-mentioned memory control means eliminate the extra sensitive information memorized by the 1st memory device while they read the information which should be saved from the 1st memory device and write it in the 2nd memory device, when the abnormalities in output voltage of a cell are detected by the voltage surveillance means. Thus, since memory control means eliminate the extra sensitive information memorized by the 1st memory device while they read the information which should be saved from the 1st memory device and write it in the 2nd memory device, when voltage change which originates in the attack [exhausting / with time / a cell] to a cell by the voltage surveillance means is detected, they can reconcile prevention of leakage of secrets and preservation of required information.

[0006]

[Embodiments of the Invention] Next, the gestalt of operation of this invention is explained in detail with reference to a drawing. Drawing 1 is the block diagram showing the composition of the carried type information-storage medium used as the gestalt of operation of this invention. The sensor element 2 as which the carried type information-storage medium 1 of the gestalt of this operation detects the physical attack from the outside, The 1st memory device 3 in which write-in read-out is possible, and the external ON appearance carport 4 for considering an exchange of data as external reader/writer, When a physical attack is detected by the 2nd memory device 5 and sensor element 2 only for read-out which can be written in only at once, Or when the abnormalities in output voltage of a cell are detected by the voltage surveillance mentioned later, while reading the information which should be saved from the 1st memory device 3 and writing in the 2nd memory device 5 It has the memory controlling mechanism 6 which eliminates the extra sensitive information memorized by the 1st memory device 3, the cell 7 for supplying power to the 1st, the 2nd memory device 3 and 5, and memory controlling mechanism 6 grade, and the voltage surveillance 8 which supervises the output voltage of a cell 7.

[0007] The sensor element 2 is a sensor which detects the physical attack (physical stimulus it is considered that are unjust actions, such as opening of a sealing agent) from the outside, and is constituted by the electronic circuitry which detects the change more than the electric resistance of the photo detector which detects the incident light to the interior by the sealing agent of a medium 1 having been opened, and a closure portion, or the specified quantity of electrostatic capacity, or the shock sensor which detects the shock more than the specified quantity. The electronic circuitry which detects change of the electric resistance of a closure portion measures the electric resistance of a metal plate established so that the composition of drawing 1 might be optically covered in a sealing agent, and detects change of the electric resistance by the metal plate having been removed by the attack from the outside. The electronic circuitry which detects change of the electrostatic capacity of a closure portion measures the electrostatic capacity between the above-mentioned metal plates which counter on both sides of a sealing agent, and detects change of the electrostatic capacity by the metal plate having been removed by the attack from the outside.

[0008] The 1st memory device 3 is memory used as work memory for temporary storage, and is constituted by non-volatile memory, such as volatile memory, such as RAM (Random Access Memory), or EEPROM (Electrically Erasable and Programmable Read Only Memory), while it memorizes extra sensitive information, such as a code key, individual authentication information and the balance, and a savings point size.

[0009] Only at once, the 2nd memory device 5 is the non-volatile memory which can be written in electrically, and is constituted by the one time PROM (Programmable Read Only Memory). A fuse is prepared in this one time PROM for every memory cell, and there is a fuse fusing type which melts a fuse in the case of data writing in it. In addition, the 2nd memory device 5 is carried in a medium 1 still in the state in the state where it does not write in.

[0010] As a memory controlling mechanism 6, you may use central processing units (CPU), such as a memory management unit (MMU) of a computer, and a microprocessor, for example. Next, operation when the carried type information-storage medium 1 of the gestalt of this operation receives the attack from the outside is explained. Drawing 2 is the flow chart view showing operation at the time of a medium 1 receiving an attack.

[0011] When a physical attack is detected by the sensor element 2, or when the abnormalities in output voltage of a cell 7 are detected by the voltage surveillance 8 (drawing 2 step 101), the memory controlling mechanism 6 reads the information which should be saved [point size / savings / the balance,] from the storage region of the extra sensitive information in the 1st memory device 3, and writes the read information in the 2nd memory device 5 (Step 102). Then, the memory controlling mechanism 6 eliminates extra sensitive information by rewriting to the storage region of the extra sensitive information in the 1st memory device 3 (Step 103).

[0012] As mentioned above, by the carried type information-storage medium 1 of the gestalt of this operation, since

extra sensitive information is eliminated when a physical attack is detected, or when the abnormalities in output voltage of the cell 7 by exhausting [a cell 7 / exhausting / removal or] are detected, decode of extra sensitive information can be made impossible. Moreover, about the information among extra sensitive information to be saved, the memory controlling mechanism 6 writes in the 2nd memory device 5.

[0013] For example, when the carried type information-storage medium of this invention is applied to a prepaid card, a cybermoney card, or a point card, after deleting extra sensitive information, such as a code key and individual authentication information, from the memory device 3 in a card and writing in a memory device 5 about balance data or a savings point size, it deletes from a storage region from the first. Even when a security mechanism can operate, disclosure of extra sensitive information can be prevented, when an attack is intentionally added to a card, and a security mechanism operates according to accidental accident by this, it becomes possible to save information, such as the balance.

[0014] Therefore, if the prepaid card of balance zero is destroyed intentionally, since it is recorded on the 2nd memory device 5 of this card that the balance is zero and the information on the memory device 5 which can moreover be written in only at once cannot be rewritten, it can prevent those who destroyed the card of balance zero intentionally reporting themselves as the card became poor, and converting into money unlawfully. Moreover, it can be checked whether since the writing to the 2nd memory device 5 was performed when the card was opened, when checking the write-in state of the 2nd memory device 5, the attack has been added to a card. Therefore, it becomes possible to judge whether it is the card which suffered damage though the card was closed and the normal card was pretended after opening a card unjustly.

[0015] In addition, the capacitor which is not illustrated is arranged in parallel by the cell 7, and drawing 2 can be operated even when a cell 7 is removed by the charge stored in this capacitor. Moreover, the carried type information-storage medium 1 of this invention may be the gestalt of the IC card which embedded the semiconductor chip on the card made of a resin, and may be the gestalt of PCMCIA (PC card) which built thin shape parts into the thin shape case. Moreover, the composition which could constitute the sensor element 2, memory devices 3 and 5, the memory controlling mechanism 6, and the voltage surveillance 8 from independent parts, and was accumulated on one chip may be used.

[0016]

[Effect of the Invention] According to this invention, the unjust attack and the accidental accident from the outside, exhaustion of a built-in cell, etc. are interlocked with by preparing a sensor element, the 1st memory device, the 2nd memory device, and memory control means in claims 1 and 2 like a publication, and since elimination of extra sensitive information and the information which should be saved are held, prevention of leakage of secrets and preservation of required information can be reconciled. If this carrying type information-storage medium is unjustly opened for analysis of operation or decode of storage information, since extra sensitive information will be eliminated immediately, the format of an encryption procedure, a code key, and a storage region etc. can protect information important for decode from disclosure. Since the extra sensitive information currently written in the 1st memory device though the information written in the 2nd memory device was decoded is eliminated, it becomes impossible to restore original extra sensitive information. If the carried type information-storage medium it became impossible to use by exhaustion of accidental accident and a built-in cell is brought to the management engine of service when this carrying type information-storage medium is applied to a prepaid card or a point card, information required for a new carried type information-storage medium can be copied. Moreover, it can judge whether it is the medium which suffered damage by checking the write-in state of the 2nd memory device, though it recloses after those who destroyed the carried type information-storage medium of balance zero intentionally can also cope with the crime of reporting oneself as the medium became poor, and requiring illegal liquidation and open a carried type information-storage medium unjustly, and a normal medium is pretended.

[Translation done.]

DE4217444

Unofficial English Abstract

Publication date: 1992-12-03
Inventor(s): IMADA TOYOHISA (JP); TAKESHIMA YASUSUKE (JP)
Applicant(s): HITACHI LTD (JP); HITACHI COMPUTER ENG (JP)
Application Number: DE19924217444 19920526
Priority Number(s): JP19910120761 19910527
IPC Classification: G06F12/08
EC Classification: G06F9/455H, G06F12/02D
Equivalents: GB2256513, JP4348434

Abstract

A virtual machine system having a plurality of virtual machines, in which each virtual machine can be relocated to a now storage area of main storage without interfering with any other virtual machine. The relocation is carried out by move instructions issued by a service processor 5 upon receipt of a relocate command. These instructions pass control to a controlling section 6 which instructs a logical instruction processor (LIP) controlling section 7 to temporarily stop the LIP of the particular virtual machine. Next a check is made by the resource managing section 8 to determine whether the virtual machine can be moved. Once that has been checked, the virtual machine is relocated on the main storage area in accordance with a designated address by the relocate command and the controlling section 7 restores operation of the virtual machine.

Data supplied by epo database